CHAPTER

1

IDENTIFYING SECURITY RISKS

After reading this chapter and completing the exercises you will be able to:

- Identify information-technology-related security risks faced by corporations.
- Identify security risks that are internal to a corporation.
- Identify security risks that are external to a corporation.
- Identify general principals in managing security risks.

You are the network architect for a large company, and you have been given the task of designing a security plan for the entire corporation. As in most companies, the information technology (IT) infrastructure has become an essential component of doing business, and people use their computers constantly. Without the computers on every desk, without the network and the servers, without the Internet connection and e-mail, very little work would get done in your company. Again, as in most other corporations, a great deal of effort and money goes into making sure that all of the components of the IT infrastructure are available all of the time.

The news media is full of stories of security issues related to computers. Everyone has heard of incidents where crucial corporate information has been stolen from a server on the network, sometimes by people working for the organization, sometimes by people outside the organization. Almost everyone knows about **firewalls** (a security device that allows internal users access to the Internet, while restricting or blocking access from the Internet), and the need to protect the company from Internet intruders. Computer viruses have become a fact of life for most computer users, and have the potential to cost a large corporation millions of dollars in lost productivity and damaged prestige.

Often the task of protecting the IT resources in a large corporation seems to be almost insurmountable. The IT infrastructure is essential to business because it makes information easily available to people. The information may be available on an Intranet site, as a share on a server, in a public folder on a messaging server, or through some other location. One of the primary goals of the IT infrastructure is to make sure that all users have access to the data and services that they need wherever they are. However, this also makes it easier for users who should not have access to gain access. To overcome this problem, a corporate security plan has to ensure that those people who need access to information can get the right level of access, while preventing unauthorized people from accessing the data.

Designing a security plan also includes designing secure access to services on the network. Almost every company has a corporate messaging system that most users need to access. Frequently, corporations have a central line of business applications that many users in the organization must be able to use if they are to get their work done. More and more, corporations are moving to web-based applications requiring constant access to web servers. Some organizations are deploying terminal servers in central locations, and all users have to connect to these servers in order to run business applications. As with information, the protection of services is an essential component of the security plan for the corporation. If users cannot get access to a service on the network, less work gets done.

Designing a security plan with secure access to services on the network is complicated because:

- The information and services may be located in many different places.
- The information and services may be accessible in many different ways.
- The authorized users may include corporate employees, employees in partner organizations, customers, or anonymous users accessing a corporate Internet site.

When designing a corporate security plan, you need to identify the threats to your network before you can begin the planning process. This chapter provides an overview of the security risks your IT infrastructure may face.

> This chapter also introduces the rest of this book. After each discussion of a particular security risk, a note indicates the chapter or chapters in the book that deal with solutions to that security risk.

INTERNAL SECURITY RISKS

The first and most important threat to the security of your IT infrastructure is the threat that comes from inside the corporation. Often the external security risks, such as someone breaking through a firewall, have a higher profile, but much more damage is done by internal breaches of security. Some of these internal security breaches may be accidental and harmless. For example, someone in the office connects to a network share that the user should not have access to and looks at confidential information, but does not tell anyone else. Other types of internal security breaches might be much more deliberate and malicious. The person may be deliberately looking for confidential information on the network in order to sell that information to a competitor. Or a user may use an unauthorized **packet sniffer** on the network to capture data or passwords as they cross the network.

Protecting against the internal threats to your network is also the first step in dealing with external threats. For example, if you use NTFS (NT file system) security so that only authorized users can access confidential information on the server shares, you have also prevented external users from being able to access the data if they ever obtain the password for one of the unauthorized users. If your servers are locked up in a secure server room, you prevent both internal and external people from accessing the servers.

Access to Information

The first security risk is the threat that users may have access to data for which they are not authorized. In almost every company, the corporate data is stored on file servers in a central location. The servers and the access to the data on the server are centrally managed by network administrators. In some organizations, data is also stored on individual workstations, introducing a much more serious risk of unauthorized access. This is particularly true if the data is stored on a computer running an insecure operating system such as Windows 95 or Windows 98 because there is no file-level security provided by these operating systems. Even if Windows 2000 Professional is used as the corporate desktop, allowing users to store data on their desktops means that the users have to manage the security of the data, and most users do not understand the security implications or how to manage the security. In most cases, the data should be stored on a server.

Another potential area where users may get unauthorized access to data is the theft of the actual computer. This is most important when users are taking laptop computers out of the office. Often the users need to carry important data with them on the laptop, but there is the risk of losing that data if the laptop is stolen. Ideally a corporate security plan should define what data is allowed to leave the office on a laptop hard disk, as well as provide some protection for the data while it is out of the office.

Another risk to confidential data occurs when the data is printed. If the corporation's printers are located in an area that all employees can access, there is the risk of someone having access to printed copies of the confidential data. For example, someone may be printing a confidential human resource document; if this document is left at a public printer for any length of time, the confidential information may become widely known.

The amount of damage to the organization that can result from unauthorized access to data can range from minimal to extreme. If a user gets access to confidential information, but does not do anything with that information, there may be no damage. However, if one person can gain unauthorized access to the data, then there is a good chance that someone else can also access the data illegitimately, and not everyone can be trusted. In more serious cases, inappropriate access to information may result in the release of confidential, but not necessarily crucial, information. For example, most organizations would not want the payroll information or everyone's home address and phone number to become public knowledge. In a very serious situation, unauthorized access to data could result in someone inappropriately modifying the data. This can have disastrous effects on the organization. For example, someone may modify the information on a contract or change the specifications on a product. Possibly the worst case scenario for someone gaining unauthorized access to corporate data is that the person may then sell the confidential business data. This may be intellectual property such as new research information, or information concerning corporate strategies, such as plans to buy out a competitor. In these cases, the inappropriate release of information may threaten the very existence of the corporation.

Note

Chapter 3, "Securing Resources on Windows 2000" covers most of the information you will need to secure access to the data on your network.

Access to Network Traffic

Another internal threat to the network is the risk of someone capturing and reading information as it crosses your internal network. Much of the data that is sent on a network is sent in clear text. For example, with **Simple Message Transfer Protocol (SMTP)** (the protocol used to send all internet mail) mail is transmitted in clear text, as is all Hyper Text Transfer Protocol (HTTP) traffic. A person with access to your network can use a simple packet sniffer to capture the traffic on the network, perhaps gaining access to confidential information.

If a user can get access to your network and capture the traffic, the user may also be able to capture and decrypt user passwords. Windows 2000 uses Kerberos as its authentication protocol, and it is very difficult to determine user passwords by capturing a Kerberos authentication session. However, if you are using down-level clients such as Windows 95 and Windows 98, the passwords cross the network in a format that can be easily cracked using free tools that can be downloaded from the Internet. After capturing the password, the intruder can then log on as the user and gain access to all resources that the user has access to. If the captured password belongs to a network administrator, the intruder can make other changes to the network, including creating an account for themselves, or resetting another user's password and then logging on as that user.

Another potential security threat that is related to access to network traffic is the danger of man-in-the-middle (or person-in-the-middle) attacks. In this type of attack, the intruder intercepts the traffic flowing from one person to another and pretends to be the other party. As Figure 1-1 illustrates, the two legitimate computers continue to send information to each other, unaware that the data is passing through the intruder's computer. The information might simply be monitored, or it could be modified. Protecting against a man-in-the-middle attack requires some form of authentication and integrity checking, as well as encrypting the traffic on the network.

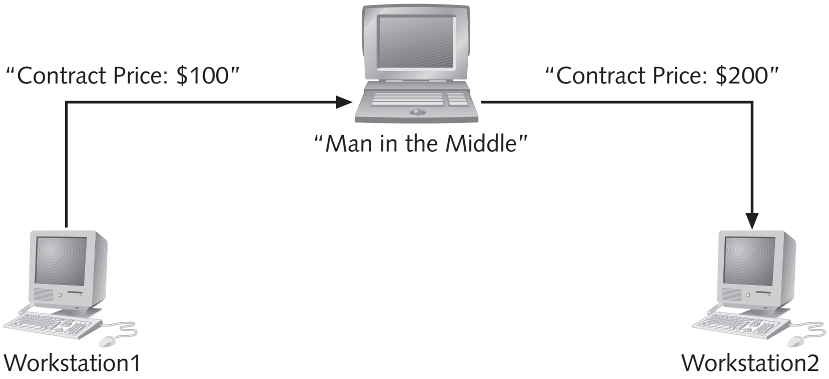

Figure 1-1 A man-in-the-middle attack

Note

Chapter 5, "Implementing a Public Key Infrastructure", Chapter 6, "Securing Network Services", and Chapter 7, "Securing Network Communications" all address different aspects of securing access to network traffic.

Access to Administrative Rights

Another serious security issue on many networks is having too many people with administrative rights. Some organizations put almost everyone into the Domain Admins group. Sometimes this is done to make it possible for the users to install software with elevated permissions on their Windows NT or Windows 2000 desktops. In some organizations, the Domain Admins group is used to give the users a high level of permissions to network resources. In other cases, a user may be added to the group for a temporary reason, and then never removed from the group.

One of the reasons for the large number of users in a powerful group like Domain Admins is the way that Windows NT domains are designed. In a Windows NT domain, the user has to have administrative rights for the entire domain in order to perform a simple task like resetting passwords for users. If a user or group is given the task of creating and managing user accounts for a particular department, the group has the same rights throughout the entire domain. Because Windows NT does not support any granularity of permissions within a domain, many organizations create additional domains, or have many people with domain administrator rights.

If too many people have administrative rights, the network will never be secure. For example, Domain Admins can put themselves or other people into any Active Directory group and assign that group any level of permission to any object in Active Directory, or full access to any file on an NTFS partition. A domain administrator can take ownership of all objects in Active Directory or on an NTFS partition, and as the owner, the administrator has full control of the object. The domain administrator can also reset any user's password, and then log in as that user. If security logging is enabled on the network, the administrator can clear the security log, thus eliminating any evidence of inappropriate activities.

The potential damage that comes from having too many people with a high level of permissions is limitless. The domain administrator may assign permissions to objects or put the wrong people into groups without understanding the full security implications of the action. As a domain administrator, the user has full access to all objects in the Active Directory domain and might delete objects accidentally or intentionally, possibly creating a problem that could take weeks to repair. The domain administrator might also step outside the realm of his or her expertise. For example, the Domain Admins group is automatically added to the administrator's local group on every server that is a member of the domain. This list of servers might include a Structured Query Language (SQL) server running a business-critical application. A domain administrator without proper training in administering the SQL server can do a great deal of damage to the server.

Chapter 4, "Designing Active Directory for Security" details how Windows 2000 Active Directory can be used to deal with many of these administrative security issues. One of the biggest advantages of Windows 2000 over Windows NT is this ability to delegate administrative tasks in a granular manner. Chapter 6, "Securing Network Services" explains how to use security templates to enhance the security on network servers.

Access to Network Services

As the IT infrastructure has grown in importance in most organizations, the amount of equipment required to support critical network services has increased greatly. This equipment includes messaging servers, database servers operating as the backend for a critical business application, a web server, or a terminal server. As a result of the importance of network services, a serious security concern is the threat of not being able to access the service. Sometimes the loss of the service is due to some component failure. For example if the server running the service fails, users will not be able to access the service. Or if a router shuts down, those users that access the service through the router will not be able to connect.

The security threat that is associated with a loss of access to network services is called a **denial-of-service (DoS) attack**. A denial-of-service attack is any kind of attack on the server that prevents legitimate users from being able to access a service. One form of a denial-of-service attack occurs when one or more computers are used to bombard a server or service with so much traffic that legitimate traffic cannot get through. For example, if you are using an internal web site to make corporate information easily available to users in the corporation, a denial-of-service attack can disable the web server so that it is not accessible to legitimate clients. This type of attack will probably not result in the theft of information or any permanent damage to your network, but it can cause significant inconvenience and perhaps a loss of trust and prestige if it happens at the wrong time.

DoS attacks usually cause loss of access to network services in three ways: by consuming bandwidth, by consuming resources, and by taking advantage of flaws within an application or operating system. A DoS attack that consumes bandwidth uses up all of the available bandwidth for the attack, thus blocking any legitimate traffic from using the network connection. An example of such an attack is a program called Smurf, which uses a flood of ICMP (Internet Control Message Protocol) packets to consume all available bandwidth. As Figure 1-2 illustrates, an attacker might use several computers on fast network connections to send packets to a single network connection to the web server, thus using up all of the available bandwidth.

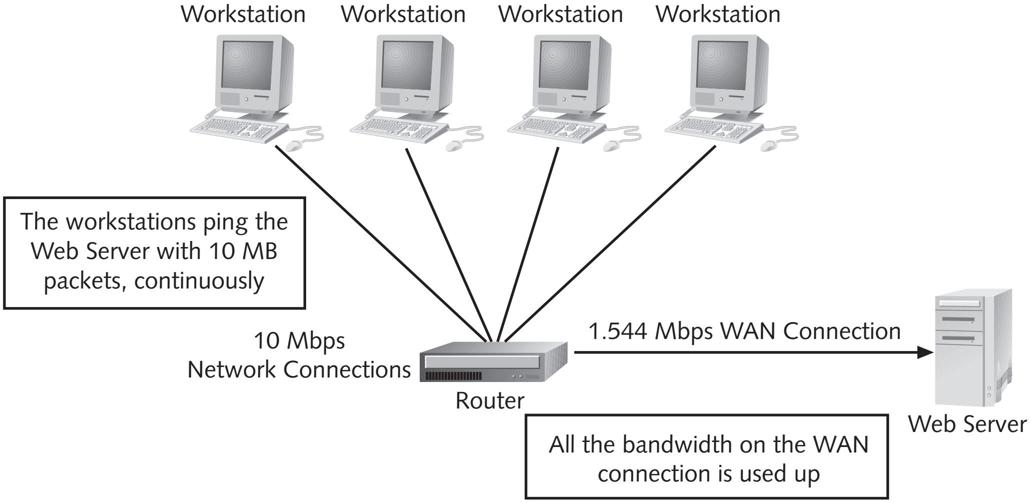
Workstation
Workstation
Workstation
Workstation
The workstations ping the Web Server with 10 MB packets, continuously
10 Mbps Network Connections
Router
1.544 Mbps WAN Connection
Web Server
All the bandwidth on the WAN connection is used up

Figure 1-2 A bandwidth consumption Denial-of-Service attack

A DoS attack that consumes all of the server resources prevents legitimate clients from accessing the server. For example, an attack on a Web Server might consume all of the system resources (such as CPU [central processing units] cycles, or memory) so that other users cannot access the web site. If the server is providing other services on the network, these services are blocked as well. In some cases, server resources are used up during the attack; in other cases, the attack can cause the system to crash.

The third type of DoS attack takes advantage of programming flaws in either an application or the operating system itself. Operating systems, applications, or even CPUs are never completely free of flaws, and over time, hackers usually find the flaws that exist. A common example is when a hacker uses non-standard TCP/IP packets, or sends extremely large packets to the server, causing a buffer overrun. The attack may cause the server to crash, or it may create an opportunity for the hacker to run another application on the server, often with a high level of privilege on the system.

One of the most destructive DoS attacks currently is not an attack at all, but rather an e-mail virus attack. This type of virus is usually sent as an attachment to an e-mail user, and when it is opened, it scans through the client's address list, and then forwards a copy of the virus to everyone in the address list. This type of attack is not set up as a standard DoS attack, but it has the same effect. For example, the Melissa virus paralyzed many large networks around the world for days by sending millions of e-mail messages through the system.

The effect of DoS attacks can range from being a nuisance to causing serious damage. If a hacker blocks access to your web site for a short period of time, you will be upset, but little permanent damage will probably have been done. If the hacker blocks access to your web site for an extended period of time when you are doing a corporate promotion on your web site, your company may lose a great deal of money, as well as suffer loss of prestige. If the hacker manages to gain control of your server through a buffer overflow attack, the damage may be much more serious if that enables the hacker to attack your internal network.

Note

Protecting your network from DoS attacks is very difficult. If a user has legitimate access to a service on your network (like a web server) or has access to your network at all, launching a DoS attack is not that difficult. Chapters 6 through 10 all deal with topics that will be important in dealing with DoS attacks. Other methods of protecting against this type of attack include working together with your ISP (Internet service provider) to block DoS attacks before they get to your network. Maintaining a good antivirus policy is also essential in protecting your network.

External Security Risks

The second important threat to your organization is the threat that comes from the outside. Most high-profile attacks are launched from outside the organization. As mentioned earlier, the e-mail virus attack has gained a huge amount of publicity. Everyone has heard of cases where a hacker managed to break into a corporate network and steal confidential information. Several high-profile denial-of-service attacks have been launched against corporations doing business on the Internet.

Access to the Internal Network

One of the highest profile and most dangerous attacks is when a hacker manages to get access to the internal network from the outside. The most dramatic of these attacks is when a hacker circumvents a firewall and gets access to the internal network. In this type of attack, the hacker either exploits a known weakness in a firewall or takes advantage of an incorrectly configured firewall to gain access to the internal network. Once the hacker has achieved this access, the potential damage is immense. Sometimes the hacker is interested only in humiliating the company and may deface the corporate web site to broadcast the successful attack. In other cases, the hacker may steal information. Perhaps the most insidious attack is to break through the firewall, install an application on the network that will forward internal information to the Internet, and then remove all evidence of having hacked into the network. If the application is not detected for an extended period of time, the hacker may be able to collect all of the passwords on the network or collect a great deal of corporate information.

Hacking into a corporate network through a firewall may be a high-profile crime, but it is also an extremely difficult one if the firewall is configured correctly. Most top quality firewalls can be configured to be very secure, or at least secure enough that the hacker will move on to other, easier targets. Most of the time, when a firewall is compromised, it is as a result of an incorrect configuration. In many organizations, the firewall configuration is left up to one of the network administrators who has a multitude of other tasks to perform. This means that the administrator might not have time to keep up with the latest recommended security settings, or the latest patches to the firewall. As a result, the firewall is configured in a less than secure manner.

In most cases, however, the hacker will just figure out a different way to access the network. For example, one method is by using a practice called **social engineering**. This type of practice exploits the weakest part of any IT security system—the people who manage or use the network. A typical example of social engineering is for a hacker to call a user (or send the person an e-mail, or some other form of communication) and pretend to be someone with authority on the network. For example, a person may call the help desk and pretend to be the IT manager. Or a person may pretend to be working at the help desk and call a regular user. The purpose of social engineering is to trick the user into giving out confidential information (usually the user's logon name and password) or to trick the user into changing the password to a value known by the hacker. Once the hacker has access to the password, the information will be used to gain access to the network, perhaps through a virtual private network (VPN) connection or dial-up remote access.

Dial-up remote access service (RAS) servers are often points of attack on a network. In order for users to use RAS, you have to make the RAS server available through a phone and modem connection. Other than your firewall, this may be the only direct point of access to your network from the outside, and most organizations spend much less time worrying about security on the RAS server than they do on the firewall. Most organizations receive a consecutive series of phone numbers from the phone company and then just assign some of these numbers to the RAS server. By looking at the list of phone numbers the company makes available, the hacker can often very quickly identify the RAS phone numbers and then begin the attack. Often the RAS attack is combined with a social engineering attack, where the hacker will acquire the user name and password of a person who has permission to dial in. Then the hacker will attack the network through the RAS connection. Sometimes the hacker can get access to the user names and passwords of former employees and then determine whether the accounts have been disabled. (Sometimes a security audit for a company will reveal that people who were fired a few years earlier still have permission to dial into the RAS server.)

Note

Protecting your internal network from external attack is a complicated task. One of the first steps is to install a good firewall. Chapter 10, "Designing Secure Access to the Internet" covers some of the basic principles of firewall configuration. Chapter 8, "Securing Access for Remote Access Users" identifies ways to prevent hackers from exploiting your RAS servers. In addition, many of the principles that deal with protecting your network from internal attacks also apply to external attacks. If the NTFS permissions on your file system are configured correctly, the hacker will have to get the user name and password of a user that has correct permissions before they will be able to get access to data. If the network traffic is encrypted by using **Internet Protocol Security (IPSec)**, then even if the hacker can launch a packet sniffer on the network, none of the captured traffic will be readable.

Sending Information on Public Networks

The second type of external attack has nothing to do with a hacker breaking into your network, but rather with the exposure of your data to possible attack when you are sending it across a public network. Most corporations are sending a great deal of information through the Internet and most of the information is sent in clear text. For example, many people send Internet e-mail without being aware that almost all SMTP mail is sent on the Internet in clear text. Many corporations now provide access to corporate messaging servers through a web interface. Again, unless the corporation has configured the Web server to encrypt the traffic, all of the mail is sent as an HTML document, which means that the messages are sent in clear text.

It is very difficult to require that all of the traffic sent from your office on the Internet be encrypted. Most organizations are not set up to encrypt SMTP traffic, so if you are going to insist that all of your SMTP traffic must be encrypted, then you will not be able to send or receive mail from those organizations. However, you can force encryption of some of the most important and confidential traffic. For example, some organizations are starting to use the Internet as an interoffice Wide Area Network (WAN) connection. With the advent of cable modems and Digital Subscriber Line (DSL) connections, relatively fast access to the Internet has become easily affordable for most companies, so using the Internet as the WAN connection can be inexpensive and rapid. Encrypting this traffic between the corporate locations is also quite easy to set up by creating a VPN (Virtual Private Network) through the Internet. Because both sides of the connection are under the control of the same company, it is easy to enforce rules so all of the traffic that is passed between the locations will be encrypted.

Note

However, for a great deal of information you send on the Internet, you do not have direct control of both parties in the traffic flow. Most organizations are now doing some type of business on the Internet, and customers or partner organizations need access to data that may exist on the corporate network. Customers may also provide the company with data (like credit card information) that must be kept confidential. To provide the required protection for this type of traffic, you will have to implement some way to authenticate the users of your services, as well as some way to encrypt the data that is sent between the computers on the network.

Note

Chapter 5 details the planning and implementation of a **Public Key Infrastructure (PKI)** that is needed to create the certificates and public and private keys used to encrypt traffic on the Internet. Chapter 9, "Securing Access Between Corporate Locations" describes how to ensure that all data sent between corporate locations is protected.

Managing Security Risks

Obviously there are many threats to the security of your IT infrastructure, both internal to the organization and from outside of the organization. As a person in charge of protecting the network resources, you are faced with numerous threats and even more options for dealing with the threats. This book details many options for protecting your Windows 2000 network, but as you look at all the options, you will find that you need to keep in mind some general principles.

First of all, designing a secure network is almost always a question of balancing two or more options. For example, it is important to consider the question of risk versus threat. The first step in designing a security policy is to evaluate the threat. If you are working for Microsoft or the IRS, the threat to your network is huge, so you will have little room for any kind of a risk. If you are working for one of the millions of small, almost invisible organizations, the threat to your network is probably much less, meaning that you have more room for risk. If you don't have anything worth stealing, you don't have to work quite as hard to protect it. This is not to say that you don't have to worry about security, it is just that the threat is much lower.

When designing a security plan, it is also essential to consider the need for security versus the need for accessibility. You may be able to design an almost impregnable security plan, but if that plan prevents the users in the corporation from being able to do their work, or if it makes it significantly more difficult for the users to do their work, your security plan will not be well accepted. For example, the only way to have a completely secure connection to the Internet is not to have one. If you disconnect your network from the Internet, then no one will ever be able to break into your office network from the Internet. However, if your company requires Internet access in order for the users to get their work done, then this is obviously not an ideal solution. Here is another example: A good security policy requires long complex passwords that have to be changed frequently. If you enforce this policy, you may find that many users are writing down their passwords and hiding them under their mouse pads. Or you may find that you are spending a large amount of time resetting user passwords. Ultimately, your IT infrastructure is useful only if it allows user access to the data and services they need. A good security policy should not prevent them from getting this access.

Another essential aspect to designing a security policy is to maintain a clear channel of communication between the people who are designing the security policy and the people who will be affected by the policy. As you collect the information about your organization that you will need to design an effective policy, keep the users informed about what you are doing and why. As you prepare to implement the security policy, you will need support from corporate management to enforce the policy. Implementing a new policy usually means change, and people can be strongly resistant to change if they do not see the need for it. Something as simple as a password policy change increasing the complexity requirements for a password can cause considerable disruption within the company. Sometimes the resistance to change comes from purely personal reasons, but sometimes resistance arises from excellent business reasons. Before doing any planning, make sure you have collected all of the relevant information, and keep the people affected by the policy informed.

For most organizations, it is not very difficult to deal with the majority of the security threats. The rest of this book describes how to secure your Windows 2000 network from both internal and external attacks. It is almost impossible, however, to absolutely guarantee that your network security will never be broken. Even the most secure organizations in the world occasionally have their security breached. An essential component of designing and implementing a security policy is vigilance. Your network may be as secure as you can make it today, but someone may figure out a new way to attack your network tomorrow. One of your tasks as the security expert will be to constantly monitor the new attacks, and the new ways to protect yourself from those attacks. Another aspect of vigilance is constant monitoring of your security configuration. You may have auditing turned on so that you can monitor all the people who access a particular file, but if you never check the audit logs, the auditing is of little use. You may be monitoring your firewall for various types of attacks, but if you don't check the logs on the firewall, you may not know that an attack has occurred until it is too late. Designing and implementing a security plan for an organization is an essential first step in protecting that organization's network resources, but without constant attention, that security plan will likely soon be out of date.

Chapter Summary

- The most prevalent threats to security for most organizations are the internal risks. These risks include users with incorrect permission to access data on a network server, users capturing information as it crosses the network (including the capture of data and passwords), users with inappropriate administrative permissions, and the threat of denial-of-service attacks.

- Most organizations also face external threats to the security of the network. These threats include the danger of a hacker gaining access to the network, either by figuring out a way to get through the firewall, or by some other means such as social engineering or attacking an RAS server. In addition, when an organization sends any kind of data across an Internet connection, either through SMTP mail, a Web server, or between corporate locations, there is a threat that the information could be captured and read.

- Developing a security plan is always a question of balance. When developing the plan, you must balance the threat versus the risk, you must balance the need for high security with the need for users to easily access the data, and you must consider the cost of providing maximum security. As well, as you design your security plan, keep the users who will be affected by the plan informed, and monitor your security configuration on an ongoing basis.

KEY TERMS

denial-of-service (DoS) attack — Any type of attack on a network service that results in legitimate users of that service not being able to access the service.

firewall — A device that is located between a corporation's internal network and the Internet. It is designed to allow internal users to access the Internet while restricting or blocking access from the Internet to the internal network. A firewall may be a dedicated hardware device or an application that runs on a computer.

Internet Protocol Security (IPSec) — A method of encrypting the packets that are sent on the network between two computers.

packet sniffer — A tool that can be used to capture all of the packets that are sent on a network. The packets can then be analyzed for data or passwords.

Public Key Infrastructure (PKI) — A system of protecting data that is sent across a public network such as the Internet by authenticating and validating users and by encrypting traffic on the network. The components that make up a PKI include certificate authorities, certificates, and public and private keys.

Simple Mail Transfer Protocol (SMTP) — The protocol used to send all Internet mail. The primary security concern with SMTP is that all e-mail sent with SMTP is sent in clear text.

social engineering — A method used by people attacking the network. The attacker convinces legitimate users on the network to provide the attacker with confidential information such as logon names and passwords.

REVIEW QUESTIONS

1. Which of the following is *not* a reason why the job of corporate security office can be very complex?

   a. Almost everyone requires a computer to perform work.

   b. Computers have become more powerful.

   c. Users need access to information from a wide variety of locations.

   d. Many users now travel with laptop computers.

2. The most common type of security breach is:

   a. a hacker breaking through the corporate firewall

   b. a social engineering attack

   c. an internal attack by a corporate employee

   d. an internal attack by a domain administrator

3. A denial of service attack occurs when:
   a. All of the bandwidth going to a web server is used up with non-business traffic.
   b. An e-mail server is shut down due to a service failure.
   c. A SQL server cannot respond to client requests because too many clients are requesting information at the same time.
   d. A user cannot get access to a file because they do not have permission.
4. Which of the following is *not* a denial of service attack?
   a. using up all of the bandwidth going to a server
   b. overloading a service by sending too many requests to the service
   c. taking advantage of a flaw in the server program
   d. stopping someone from accessing the internal network by setting up a firewall
5. A social engineering attack occurs when:
   a. An attacker uses a downloaded hacking tool to try to break through a firewall.
   b. An attacker tries to get confidential user information by pretending to be a person with authority on the network.
   c. An attacker keeps trying to access confidential files on the network by guessing passwords.
   d. An attacker tries to get access to the network by dialing the company RAS servers.
6. Which of the following is *not* a potential security risk that a corporation faces if too many people are in the Domain Admins group?
   a. The Domain Admins can take ownership of any object in Active Directory and change the properties of the object.
   b. The Domain Admins can take ownership of any file on an NTFS partition on any computer in the domain.
   c. The Domain Admins group can put themselves into any security group in the Active Directory domain.
   d. The Domain Admins group can find out everyone's password and then log on as any user.
7. Many organizations have too many people with Domain Admins rights because:
   a. The organizations have upgraded from Windows NT.
   b. A user needs Domain Admins rights in order to change anything in Active Directory.
   c. Only the Domain Admins group can install software on any Windows 2000 Professional computer.
   d. Everyone is in the Domain Admins group by default.

8. One of the ways to increase the security of your network is to implement IPSec. How will this make your network more secure?
   a. IPSec makes file shares more secure.
   b. IPSec can protect your web server from attack.
   c. IPSec protects the traffic on the network so that it cannot be captured and read.
   d. IPSec can be used to limit the number of people in the Domain Admins group.
9. SMTP is the protocol used to send virtually all Internet e-mail. What is the primary security concern with using SMTP to send mail?
   a. All the mail is sent in clear text.
   b. Nobody knows how to set up secure SMTP servers.
   c. Using SMTP weakens your firewall configuration.
   d. SMTP is a new protocol and all of the security problems have not yet been fixed.
10. Most organizations enforce a policy of requiring all users to save all company data on a central file server. Which of the following is *not* a security benefit of enforcing this policy?
    a. You can centrally manage the permissions on the data.
    b. One group of administrators has the job of managing the servers and data.
    c. The data is easier to back up.
    d. You will require more hard disk space on the servers.
11. A man-in-the-middle attack creates a security risk because:
    a. No data can flow between two computers.
    b. The data might be altered as it travels between two computers.
    c. The firewall will be less effective in this situation.
    d. Users can be convinced to give their passwords over the phone.
12. Which of the following is *not* a security risk associated with a denial of service attack?
    a. Legitimate traffic may not get through to the server.
    b. The attacker will get access to user passwords.
    c. Legitimate users may not be able to access a network service that they require in order to do their work.
    d. The corporation's prestige may be damaged.
13. Which of the following is *not* a network access point that an attacker might use to get access to a corporate network?
    a. dial-up remote access server
    b. through the firewall
    c. through a VPN connection
    d. through a fax machine

14. Many companies are looking at using the Internet as a WAN link connecting company locations because:
    a. The Internet is very secure.
    b. Almost every company now has an Internet presence.
    c. Relatively fast and inexpensive Internet connections are available.
    d. These connections are very easy to set up.
15. Creating a virtual private network through the Internet has the advantage of:
    a. encrypting all of the data that is sent across the VPN
    b. making the firewall more secure
    c. increasing the download speed on the Internet
    d. encrypting all of the SMTP mail sent to the Internet
16. The primary reason why an attack on a corporate firewall succeeds is because:
    a. Firewalls cannot be secured properly.
    b. Denial-of-service attacks can break through a firewall.
    c. Firewalls are often not properly configured.
    d. Too many ports have to be left open on all firewalls.
17. A corporation that deals with very confidential information would have to spend a great deal of time and money on security because:
    a. They have more money to spend.
    b. The security risk is very high.
    c. The data will be easily available.
    d. The users at the company will not be security conscious.
18. Keeping all of the people affected by a security plan informed about the security plan is a good idea because:
    a. They are less likely to resist any changes made as a result of the security plan.
    b. It is important to get everyone's opinion on how to make the security plan better.
    c. The security plan will be easier to implement.
    d. This will make it easier for the users to defeat the security plan.
19. One of the important components to a security plan is constant monitoring of what types of information?
    a. audit logs
    b. unsuccessful logon attempts
    c. the number of hits to your web site
    d. the number of e-mail messages sent in a day

20. If you want to make sure that no one can read any information that you send to a web site:
    a. You would have to make sure that you are using the most recent web browsers.
    b. You don't have to worry about this; all data sent to a web site is secure.
    c. You would have to use IPSec to encrypt all of the traffic to the web site.
    d. You would have to use a Public Key Infrastructure to encrypt the traffic to the web site.

Setup For Hands-on Projects

The hands-on projects should meet the hardware requirements listed below:

Hardware Component	Windows 2000 Advanced Server
CPU	Pentium II 200 or higher
Memory	128 MB RAM
Disk Space	1 GB minimum for partition containing system files
Drives	CD-ROM Floppy Disk
Networking	TCP/IP 2 Network adapters Card 1 – 131.107.1.1: Label: Internal Card 2 – 131.107.2.1: Label: External Install DHCP but do not activate the scope (scope: 131.107.1.5 – 131.107.1.10) A connection to the Internet via some sort of NAT or Proxy server is assumed.

1. Install Windows 2000 Advanced server. Name the computer **Server1**.
2. Run DCPROMO to upgrade the server to a domain controller. Install DNS when prompted. Use **Lonestar.com** as the domain name. Change the zone type to **Standard Primary**.
3. For the Domain Users group, add **the right to log on locally** to the domain controllers security policy.

HANDS-ON PROJECTS

Project 1-1

In this Hands-on project, you will subscribe to the **Microsoft Security Notification Service** to ensure that you will be notified of all current security issues related to Microsoft-based software. This project assumes an Internet connection is available.

To access the Microsoft security web site:

1. With an administrator account, log on to your Windows 2000 computer.
2. Open **Internet Explorer** by double-clicking the Explorer icon on the desktop or in the taskbar.
3. In the Address Bar, type **www.microsoft.com/security**. This will take you to Microsoft's security web site.
4. To subscribe to the **Microsoft Security Notification Service**, click the **Security Bulletins** link on the navigation bar on the web page. This page lists all security bulletins previously released by Microsoft.
5. Click the link that states **Want to receive future security bulletins automatically?**
6. Follow the directions outlined on the web page to subscribe to the **Microsoft Security Notification Service**.

Project 1-2

In this Hands-on project you will check for and install any security patches that may be available for your server. This will be accomplished using the Windows Update feature of Windows 2000.

To access the Windows Update web site:

1. On the Windows 2000 Task bar, click the **Start** button. Click the **Windows Update** icon. The Windows Update web site will appear.
2. Click the **Product Updates** link to see if any updates are available for your computer. Click **Yes** to accept any component installations. A page will appear listing any critical and optional updates available based upon what is already installed on your computer.
3. Under the **Critical Updates** section, click the check box next to any updates required and click the **Download** button.
4. Read the **Download Checklist** screen and then click the **Start Download** button to begin the download and install process.
5. Reboot your computer when prompted.
6. Repeat the above process to install all security updates and service packs listed.

Project 1-3

In this Hands-on project, you will use the Internet to research some of the current security threats that security administrators should be aware of. You will then subscribe to a security-related e-mail list.

To search the Internet for security-related web sites:

1. With an administrator account, log on to your Windows 2000 computer.
2. Open **Internet Explorer** by double-clicking the **Internet Explorer** icon on the desktop or in the taskbar.
3. Click the **Search** button to open the search pane in the browser.
4. Type **network security** in the search pane and click the search button. Various security-related web sites will appear.
5. Browse various security-related links to search for any information about the most current network-related and Internet-related security issues. List the current top five security-related issues in the space below. (Sites that may be of interest are www.cert.org or www.sans.org.)
   1.
   2.
   3.
   4.
   5.
6. To subscribe to the CERT Security Advisory mailing list, in Internet Explorer type **www.cert.org** to access the CERT Security website.
7. Subscribe to the **CERT Security Advisory** mailing list by clicking the http://www.cert.org/contact_cert/certmaillist.html link on the page. This list will inform you of any critical security-related issues.

CASE PROJECTS

Case Project 1-1

Southdale Property Management manages apartment buildings for owners. The owners are individuals, groups, and investment companies using the apartment buildings as an investment.

The existing LAN is contained within a single building. There are 50 client workstations and four servers. One of the servers is a file and print server. Two servers are used for industry-specific accounting applications. The file and print server, and one of the application servers, are configured as domain controllers. The final server is used for hosting a web site and e-mail system. The web site includes a number of components: a public web site containing company information accessible to everyone, a component that is accessible only to tenants that contains tenant-related information (as well as a tenant maintenance request form), and an investors component that contains confidential investment information that should be accessible only to the current investors and potential investors who have been given a special access code to access the web page. The existing servers have just been upgraded from a single-domain Windows NT environment to Windows 2000, and the company has decided that, as part of the upgrade, overall security should be evaluated.

1. What are the most important security risks that Southside Property Management should be concerned about?
2. What security concerns might arise out of the fact that the company has just migrated from Windows NT?

Case Project 1-2

Fleetwood Credit Union is a financial services firm that serves the needs of its members in the city of Fleetwood. Its services include mutual fund sales, savings accounts, and loans. There are eight branches of Fleetwood Credit Union, including the head office where the IT staff members are located.

All eight branches of Fleetwood Credit Union are connected with a Frame Relay WAN connection that provides 128 kbps of bandwidth for each location. Each branch has 20 to 30 workstations and a single server. The main banking application is housed on a server at head office. All workstations in all branches must connect to this application when doing financial transactions. Some executives require access to the file servers from home or when traveling. To support the remote users, the company has installed a Windows 2000 server with eight dial-up modems.

All of the users at the Credit Union have access to the Internet. At this point, the branch offices do not have a direct connection to the Internet, but all Internet-bound traffic flows across the company WAN through head office to the Internet. At head office there is a single T1 connection to the Internet.

The Credit Union is also providing Internet-based services to its customers. Any customer can apply to get an online ID and then use that ID to connect to the Credit Union web site to access account information, make bill payments, and transfer money between accounts.

1. What are the most important security risks that Fleetwood Credit Union should be concerned about?
2. What additional security concerns are raised as a result of having multiple locations with WAN links connecting each location?